Guida per l'utente

AWS Client VPN

AWS Client VPN: Guida per l'utente

Table of Contents

Cos'è AWS Client VPN?

AWS Client VPN è un servizio VPN gestito, basato su cloud, che ti consente di controllare in modo sicuro l'accesso alle risorse AWS nella tua rete locale.

Questa guida fornisce le fasi per stabilire una connessione VPN a un endpoint Client VPN utilizzando un'applicazione client sul dispositivo.

Componenti

Di seguito sono riportati i componenti chiave per l'utilizzo di AWS Client VPN.

- Endpoint Client VPN: l'amministratore Client VPN crea e configura un endpoint Client VPN in AWS. L'amministratore controlla le reti e le risorse cui è possibile accedere quando si stabilisce una connessione VPN.
- Applicazione client VPN: l'applicazione software utilizzata per connettersi all'endpoint Client VPN e stabilire una connessione VPN sicura.
- File di configurazione dell'endpoint Client VPN: un file di configurazione fornito dall'amministratore Client VPN. Il file include le informazioni sugli endpoint Client VPN e i certificati richiesti per stabilire una connessione VPN. Il file viene caricato nell'applicazione client VPN scelta.

Altre risorse

Se sei un amministratore VPN client, consulta la Guida per l'amministratore di AWS Client VPN per ulteriori informazioni sulla creazione e la configurazione di un endpoint Client VPN.

Nozioni di base su Client VPN

Prima di stabilire una sessione VPN, l'amministratore Client VPN deve creare e configurare un endpoint Client VPN. L'amministratore controlla a quali reti e risorse puoi accedere quando stabilisci una sessione VPN. Puoi quindi utilizzare un'applicazione client VPN per connetterti a un endpoint Client VPN e stabilire una connessione VPN sicura.

Se sei un amministratore che deve creare un endpoint Client VPN, consulta la Guida per l'amministratore di AWS Client VPN.

Argomenti

Prerequisites

Per stabilire una connessione VPN, è necessario quanto segue:

- Accesso a Internet
- Un dispositivo supportato
- Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), uno dei seguenti browser:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

Fase 1: ottenere un'applicazione client VPN

Puoi connetterti a un endpoint Client VPN e stabilire una connessione VPN utilizzando il client fornito da AWS o un'altra applicazione client basata su OpenVPN.

Il client fornito da AWS è supportato su Windows, macOS, Ubuntu 18.04 LTS e Ubuntu 20.04 LTS. Puoi scaricare il client dalla pagina Download di AWS Client VPN.

In alternativa, scarica e installa un'applicazione client OpenVPN sul dispositivo da cui vuoi stabilire la connessione VPN.

Fase 2: ottenere il file di configurazione dell'endpoint Client VPN

Devi richiedere il file di configurazione dell'endpoint Client VPN al tuo amministratore. Il file di configurazione include le informazioni sugli endpoint Client VPN e i certificati richiesti per stabilire una connessione VPN.

In alternativa, se l'amministratore Client VPN ha configurato un portale self-service per l'endpoint Client VPN puoi scaricare la versione più recente del client fornito da AWS e la versione più recente del file di configurazione dell'endpoint Client VPN. Per ulteriori informazioni, consulta Utilizzare il portale self-service.

Fase 3: Connettersi alla VPN

Importa il file di configurazione dell'endpoint Client VPN nel client fornito da AWS o nell'applicazione client OpenVPN ed esegui la connessione alla VPN. Per le fasi di connessione a una VPN, consulta i seguenti argomenti:

- Connessione mediante un client fornito da AWS
- Connessione mediante un client OpenVPN

Per gli endpoint Client VPN che utilizzano l'autenticazione di Active Directory, ti verrà richiesto di immettere il nome utente e la password. Se l'autenticazione a più fattori è stata abilitata per la directory, ti verrà anche chiesto di immettere il codice MFA.

Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), il client fornito da AWS apre una finestra del browser nel computer in uso. Ti verrà richiesto di immettere le credenziali aziendali prima di connetterti all'endpoint Client VPN.

Utilizzare il portale self-service

L'amministratore dell'endpoint Client VPN può configurare un portale self-service per l'endpoint Client VPN. Il portale self-service è una pagina Web che consente di scaricare la versione più recente del

client fornito da AWS e la versione più recente del file di configurazione dell'endpoint Client VPN. Per ulteriori informazioni sulla configurazione del portale self-service, consulta Endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN.

Prima di iniziare devi avere l'ID dell'endpoint Client VPN. L'amministratore dell'endpoint Client VPN può fornire l'ID o un URL del portale self-service che include l'ID.

Per accedere al portale self-service

1. Accedi al portale self-service all'indirizzo https://self-service.clientvpn.amazonaws.com/ oppure utilizza l'URL fornito dall'amministratore.
2. Se necessario, immetti l'ID dell'endpoint Client VPN, ad esempi, `cvpn-endpoint-0123456abcd123456`. Seleziona Successivo.
3. Immetti il nome utente e la password e scegli Sign In (Accedi). È lo stesso nome utente e la stessa password che hai utilizzato per connetterti all'endpoint Client VPN.
4. Nel portale self-service puoi effettuare le seguenti operazioni:
   - Scaricare la versione più recente del file di configurazione del client per l'endpoint Client VPN.
   - Scarica l'ultima versione del client fornito da AWS per la tua piattaforma.

Connessione mediante un client fornito da AWS

Puoi connetterti a un endpoint Client VPN utilizzando il client fornito da AWS. Il client fornito da AWS è supportato su Windows, macOS, Ubuntu 18.04 LTS e Ubuntu 20.04 LTS.

Client

- AWS Client VPN per Windows
- AWS Client VPN per macOS
- AWS Client VPN per Linux

Direttive OpenVPN

Il client fornito da AWS supporta le seguenti direttive OpenVPN:

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive

- key
- nobind
- persist-key
- persist-tun
- ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- route
- route-ipv6
- server-poll-timeout
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN per Windows

La procedura seguente mostra come stabilire una connessione VPN utilizzando il client AWS fornito per Windows. Puoi scaricare e installare il client dalla pagina Download di Client VPN AWS. Il client AWS fornito non supporta gli aggiornamenti automatici.

Indice

Requisiti

Per utilizzare il client AWS fornito per Windows, sono necessari i seguenti requisiti:

- Sistema operativo Windows 10 a 64 bit, processore x64
- .NET Framework 4.7.2 o superiore

Il client riserva la porta TCP 8096 sul computer. Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), il client prenota la porta TCP 35001.

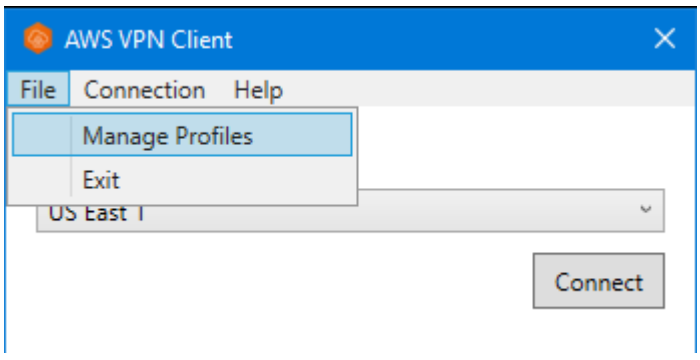
Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Connessione

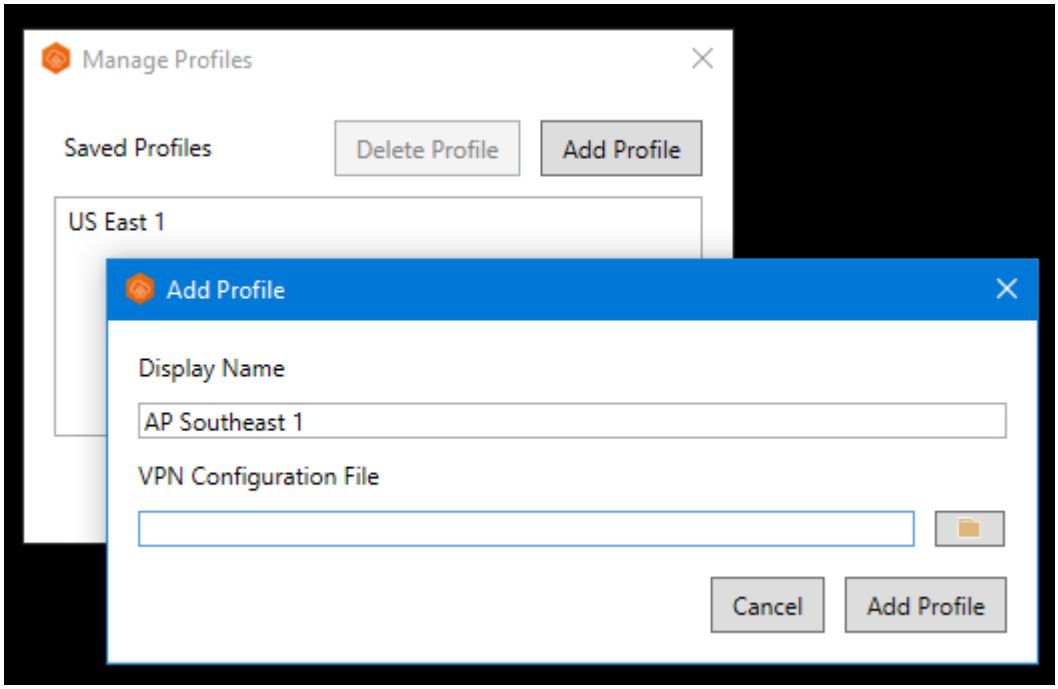
Prima di iniziare, assicurati di leggere i requisiti. Il client AWS fornito viene anche denominato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per Windows

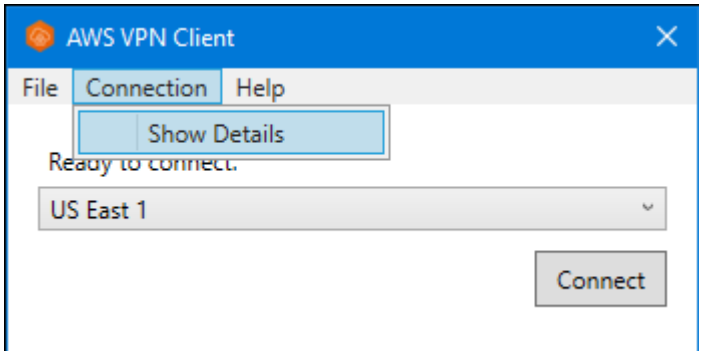
1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).



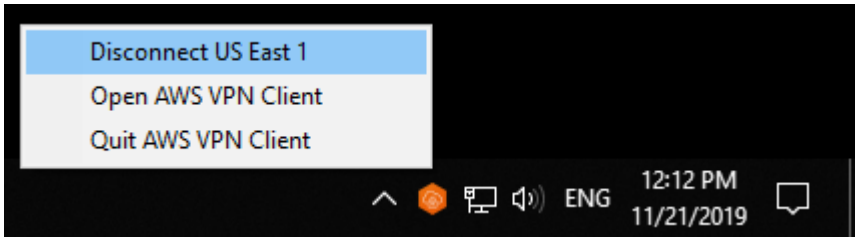
3. Scegliere Add Profile (Aggiungi profilo).



4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per VPN Configuration File (File di configurazione VPN), seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Add Profile (Aggiungi profilo).
6. Nella finestra Client AWS VPN , assicurati che il tuo profilo sia selezionato, quindi scegli Connetti . Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password.
7. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).



8. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti. In alternativa, scegliere l'icona client sulla barra delle applicazioni di Windows e selezionare Disconnect (Disconnetti).



Note di rilascio

La tabella seguente contiene le note di rilascio e i collegamenti per il download per la versione corrente e precedente di AWS Client VPN per Windows.

Versione	Modifiche	Data	Link per il download e SHA256
3.11.1	• Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.11.1 sha256: fb67b60aa837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• È stato risolto un problema di connettività causato dalle macchine virtuali Windows. • Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Versione	Modifiche	Data	Link per il download e SHA256
3.10.0	• È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. • È stato risolto un problema di connettività in presenza di adattatori di rete Hyper-V installati sul computer client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.10.0 sha256: d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.9.0 sha256: de9a3800ea2349155540bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
3.8.0	• Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.7.0	• Sono state ripristinate le modifiche rispetto alla versione 3.6.0.	15 luglio 2023	Non è più supportato
3.6.0	• Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.5.0	Miglioramenti e correzioni di bug minori.	3 aprile 2023	Non è più supportato
3.4.0	Sono state ripristinate le modifiche rispetto alla versione 3.3.0.	28 marzo 2023	Non è più supportato
3.3.0	Miglioramenti e correzioni di bug minori.	17 marzo 2023	Non è più supportato
3.2.0	• È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name». • Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni. • È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili.	23 gennaio 2023	Non è più supportato
3.1.0	Posizione di sicurezza migliorata.	23 maggio 2022	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.0.0	• Aggiunto il supporto per Windows 11. • Risolto il problema del nome del driver di Windows TAP che influenzava altri nomi di driver. • Risolto il problema del messaggio del banner che non veniva visualizz ato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato
1.3.7	• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	8 novembre 2021	Non è più supportato
1.3.6	• Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	20 settembre 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.5	Patch per eliminare file di log di Windows di grandi dimensioni.	16 agosto 2021	Non è più supportato
1.3.4	• Aggiunto il supporto per il flag OpenVPN: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato
1.3.3	• Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route. • Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita. • Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata. • Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app. • Miglioramenti e correzioni di bug minori.	1 luglio 2021	Non è più supportato
1.3.2	• Aggiungere la prevenzione delle perdite IPv6, quando è configurata. • Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione).	12 maggio 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.1	• Aggiunto il supporto per più certificati client con lo stesso oggetto. I certificati scaduti verranno ignorati. • Risolta la conservazione dei log locali per ridurre l'utilizzo del disco. • Aggiunto il supporto per la direttiva OpenVPN 'route-ipv6'. • Miglioramenti e correzioni di bug minori.	5 aprile 2021	Non è più supportato
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato
1.2.7	• Aggiunto il supporto per la direttiva OpenVPN 'cryptoapicert'. • Sono state risolte le route obsolete tra le connessioni. • Miglioramenti e correzioni di bug minori.	25 febbraio 2021	Non è più supportato
1.2.6	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato
1.2.5	• Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS.	8 ottobre 2020	Non è più supportato
1.2.4	Miglioramenti e correzioni di bug minori.	1 settembre 2020	Non è più supportato
1.2.3	Ripristina le modifiche nella versione 1.2.2.	20 agosto 2020	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.2.1	Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato
1.2.0	• Aggiunto il supporto per l'autenticazione federata basata su SAML 2.0. • Il supporto per la piattaforma Windows 7 è obsoleto.	19 maggio 2020	Non è più supportato
1.1.1	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato
1.1.0	• Aggiunto il supporto per la funzionalità OpenVPN static challenge echo per nascondere o mostrare il testo visualizzato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori.	9 marzo 2020	Non è più supportato
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato

AWS Client VPN per macOS

La procedura seguente mostra come stabilire una connessione VPN utilizzando il client AWS fornito per macOS. Puoi scaricare e installare il client dalla pagina Download di Client VPN AWS. Il client AWS fornito non supporta gli aggiornamenti automatici.

Indice

Requisiti

Per utilizzare il client AWS fornito per macOS, è necessario quanto segue:

- macOS Big Sur (11,0), Monterey (12,0) o Ventura (13,0).
- Compatibile con il processore x86_64.
- Il client riserva la porta TCP 8096 sul computer.
- Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), il client prenota la porta TCP 35001.

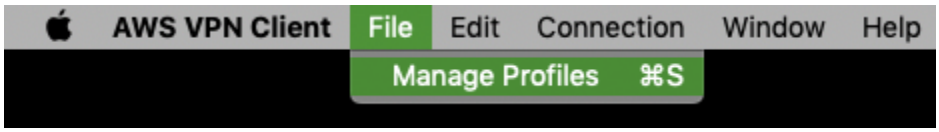
Connessione

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

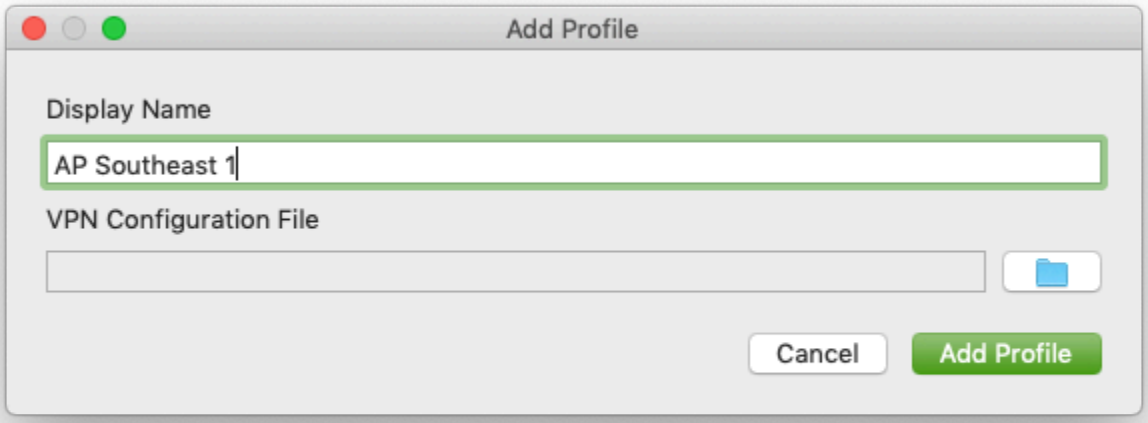
Assicurati, inoltre, di leggere i requisiti. Il client AWS fornito viene anche chiamato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per macOS

1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).

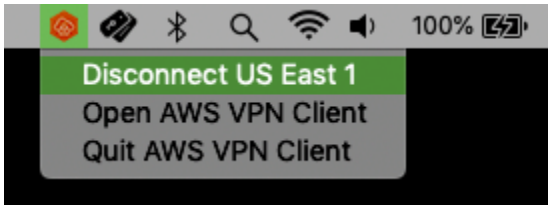


3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.



5. Per VPN Configuration File (File di configurazione VPN) seleziona il file di configurazione ricevuto dall'amministratore Client VPN. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).
7. Nella finestra Client AWS VPN assicurati che il tuo profilo sia selezionato, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password.
8. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).

9. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti. In alternativa, scegli l'icona del client nella barra dei menu, quindi scegli Disconnetti **<** **>** your-profile-name.



Note di rilascio

La tabella seguente contiene le note di rilascio e i link per il download AWS Client VPN per la versione corrente e precedente di macOS.

Versione	Modifiche	Data	Collegamento per il download
3.9.1	• Barra di avanzamento del download dell'aggiornamento dell'applicazione fissa. • Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.9.1 sha256:9bba4b27a635e75038703e2cf4cd814aa75306179fac8e500e2c7af4e899e971
3.9.0	• Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.8.0 sha256:d5a229b12efa2e88627127a6dc2

Versione	Modifiche	Data	Collegamento per il download
			7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.7.0 sha256: 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a
3.6.0	• Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.5.0	• Sono state ripristinate le modifiche rispetto alla versione 3.4.0.	15 luglio 2023	Non è più supportato
3.4.0	• Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato
3.3.0	• Aggiunto il supporto per macOS Ventura (13.0). • Miglioramenti e correzioni di bug minori.	27 aprile 2023	Non è più supportato

Versione	Modifiche	Data	Collegamento per il download
3.2.0	• È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name». • Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni. • È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili.	23 gennaio 2023	Non è più supportato
3.1.0	• È stato aggiunto il supporto per macOS Monterey. • È stato risolto il problema di rilevamen to del tipo di unità. • È stata migliorata la posizione di sicurezza.	23 maggio 2022	Non è più supportato
3.0.0	• Risolto il problema del messaggio banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato.
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.4.0	• Aggiunto il monitoraggio del server DNS durante la connessione. Se non corrispondono alle impostazioni della VPN le impostazioni verranno riconfigurate. • In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	9 novembre 2021	Non è più supportato.
1.3.5	• Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	20 settembre 2021	Non è più supportato.
1.3.4	• Aggiunto il supporto per il flag OpenVPN: dhcp-option. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.3	• Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route. • Risolto un problema legato ai nomi dei file di configurazione con spazi o Unicode. • Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita. • Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata. • Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app. • Miglioramenti e correzioni di bug minori.	1 luglio 2021	Non è più supportato.
1.3.2	• Aggiungere la prevenzione delle perdite IPv6, quando è configurata. • Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione). • Aggiungere la rotazione dei log del daemon.	12 maggio 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.1	• Aggiunto il supporto per macOS Big Sur (10.16). • Risolto un problema che eliminava le impostazioni DNS configurate da altre applicazioni. • Risolto un problema che si presentav a durante l'utilizzo di un certificato non valido per l'autenticazione reciproca che causava problemi di connessione. • Aggiunto il supporto per la direttiva OpenVPN 'route-ipv6'. • Miglioramenti e correzioni di bug minori.	5 aprile 2021	Non è più supportato.
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato.
1.2.5	Miglioramenti e correzioni di bug minori.	25 febbraio 2021	Non è più supportato.
1.2.4	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato.
1.2.3	• Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS. • Risolto un bug di disinstallazione che interessava alcuni utenti.	8 ottobre 2020	Non è più supportato.
1.2.2	Miglioramenti e correzioni di bug minori.	12 agosto 2020	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.2.1	• Aggiunto il supporto per la disinstal lazione dell'applicazione. • Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato.
1.2.0	• Aggiunto il supporto per l'autenticazione federata basata su SAML 2.0. • Aggiunto il supporto per macOS Catalina (10.15).	19 maggio 2020	Non è più supportato.
1.1.2	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato.
1.1.1	• Corretto un problema di risoluzione DNS. • Corretto un problema di arresto anomalo dell'app causato da connessio ni più lunghe. • Corretto un problema MFA.	2 aprile 2020	Non è più supportato.
1.1.0	• Aggiunto il supporto per la configura zione DNS macOS. • Aggiunto il supporto per la funzional ità OpenVPN static challenge echo per nascondere o mostrare il testo visualizz ato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori.	9 marzo 2020	Non è più supportato.
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato.

AWS Client VPN per Linux

Le seguenti procedure mostrano come installare il client AWS fornito per Linux e stabilire una connessione VPN utilizzando il client AWS fornito. Il client AWS fornito per Linux non supporta gli aggiornamenti automatici.

Indice

Requisiti

Per utilizzare il client AWS fornito per Linux, è necessario quanto segue:

- Ubuntu 18.04 LTS o Ubuntu 20.04 LTS (solo AMD64)

Il client riserva la porta TCP 8096 sul computer. Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), il client prenota la porta TCP 35001.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Installazione

Esistono diversi metodi che possono essere utilizzati per installare il client AWS fornito per Linux. Utilizza uno dei metodi forniti dalle seguenti opzioni. Prima di iniziare, assicurati di leggere i requisiti.

Opzione 1: installazione tramite repository dei pacchetti

1. Aggiungi la chiave pubblica AWS VPN Client al tuo sistema operativo Ubuntu.

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. Usa il comando applicabile per aggiungere il repository al tuo sistema operativo Ubuntu, a seconda della versione di Ubuntu:

   Ubuntu 18.04

   ```
   echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
    ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
   ```

   Ubuntu 20.04

   ```
   echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
    ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
   ```

3. Utilizza il comando riportato di seguito per aggiornare i repository del sistema.

   ```
   sudo apt-get update
   ```

4. Usa il seguente comando per installare il client AWS fornito per Linux.

   ```
   sudo apt-get install awsvpnclient
   ```

Opzione 2: installazione tramite il file del pacchetto .deb

1. Scarica il file .deb da Download di Client VPN AWS o utilizzando il seguente comando.

   ```
   curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
    awsvpnclient_amd64.deb
   ```

2. Installa il client AWS fornito per Linux utilizzando l'`dpkg`utilità.

   ```
   sudo dpkg -i awsvpnclient_amd64.deb
   ```

Opzione 3: installazione del pacchetto .deb tramite Ubuntu Software Center

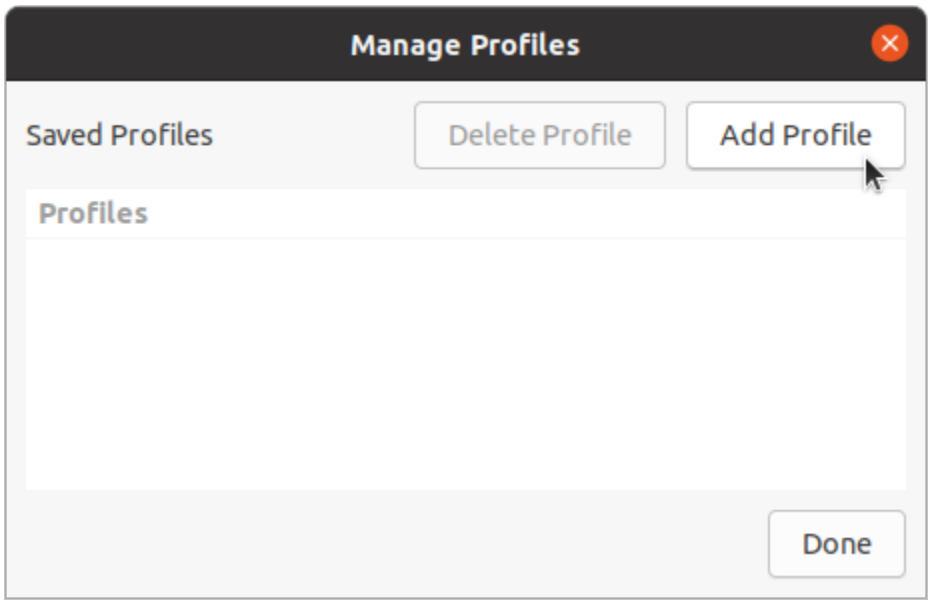
1. Scarica il file del pacchetto .deb da Download di Client VPNAWS.
2. Dopo aver scaricato il file del pacchetto .deb, utilizza Ubuntu Software Center per installare il pacchetto. Segui i passaggi per l'installazione da un pacchetto .deb autonomo utilizzando Ubuntu Software Center riportati nel Wiki Ubuntu.

Connessione

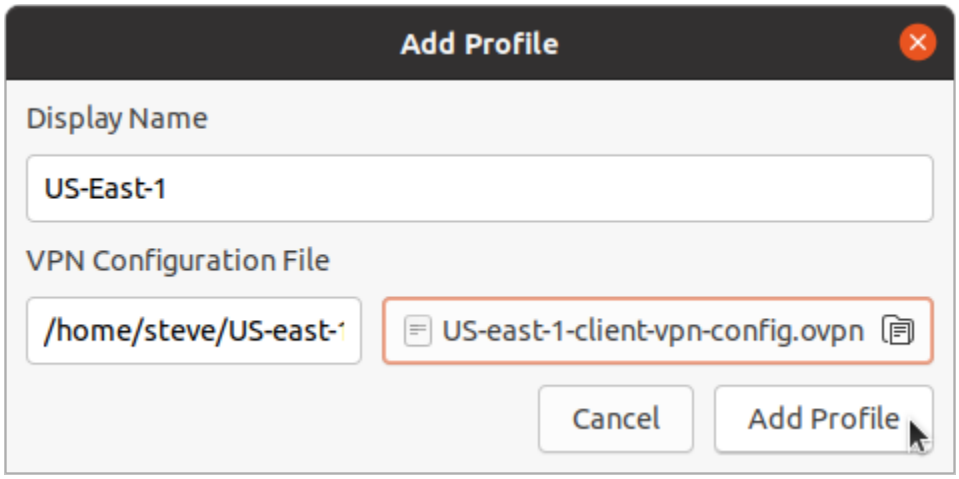
Il client AWS fornito viene anche chiamato AWS VPN Client nei passaggi seguenti.

Per connettersi utilizzando il client AWS fornito per Linux

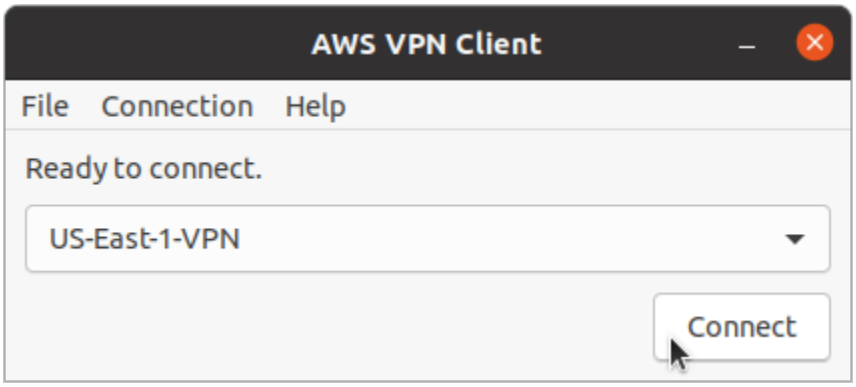
1. Apri l'app Client AWS VPN .
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).



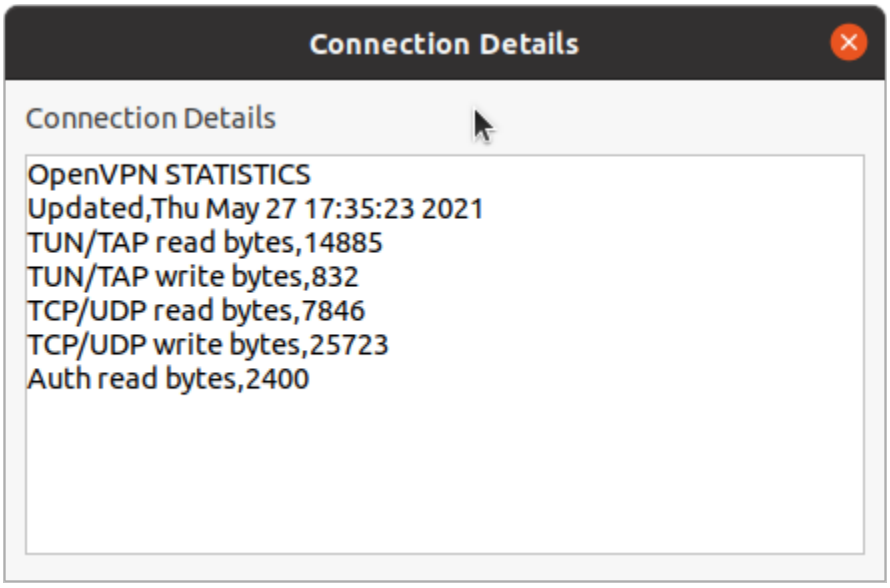
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per VPN Configuration File (File di configurazione VPN) seleziona il file di configurazione ricevuto dall'amministratore Client VPN. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).



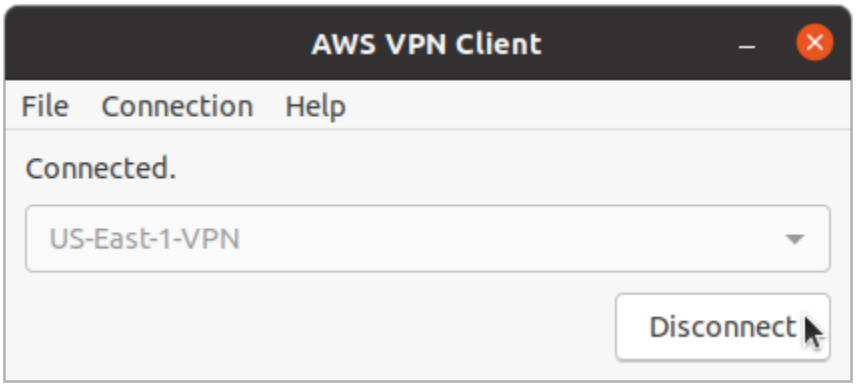
7. Nella finestra Client AWS VPN , assicurati che il profilo sia selezionato, quindi scegli Connect (Connetti). Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password.



8. Per visualizzare le statistiche della connessione, scegliere Connection (Connessione), Show Details (Mostra dettagli).



9. Per eseguire la disconnessione, nella finestra Client AWS VPN scegli Disconnetti.



Note di rilascio

La tabella seguente contiene le note di rilascio e i link per il download per la versione corrente e precedente di AWS Client VPN for Linux.

Versione	Modifiche	Data	Collegamento per il download
3.12.1	• Posizione di sicurezza migliorata.	16 febbraio 2024	Scarica la versione 3.12.1 sha256:547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• Problemi di connettività risolti per alcune configurazioni LAN.	19 dicembre 2023	Scarica la versione 3.12.0 sha256:9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1
3.11.0	• Rollback per "Problemi di connettività risolti per alcune configurazioni LAN". • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 86c0fa1bf1c97194082835a739ec7f1c87e5

Versione	Modifiche	Data	Collegamento per il download
			40194955f 414a35c67 9b94538970
3.10.0	• Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata.	6 dicembre 2023	Scarica la versione 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	• È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. • Miglioramenti e correzioni di bug minori.	24 agosto 2023	Scarica la versione 3.9.0 sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454

Versione	Modifiche	Data	Collegamento per il download
3.8.0	• Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.6.0	• Sono state ripristinate le modifiche rispetto alla versione 3.5.0.	15 luglio 2023	Non è più supportato
3.5.0	• Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato
3.4.0	• È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name».	14 febbraio 2023	Non è più supportato
3.1.0	• Risolto il problema di rilevamento del tipo di unità. • È stata migliorata la posizione di sicurezza.	23 maggio 2022	Non è più supportato

Versione	Modifiche	Data	Collegamento per il download
3.0.0	• Risolto il problema del messaggio del banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Corretta la visualizzazione del testo del banner per testo più lungo e sequenze di caratteri specifiche. • Posizione di sicurezza migliorata.	3 marzo 2022	Non è più supportato.
2.0.0	• Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori.	20 gennaio 2022	Non è più supportato.
1.0.3	• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori.	8 novembre 2021	Non è più supportato.
1.0.2	• Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf,. server-poll-timeout • Miglioramenti e correzioni di bug minori.	28 settembre 2021	Non è più supportato.
1.0.1	• Abilitata l'opzione per uscire dalla barra dell'applicazione Ubuntu. • Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route. • Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.0.0	Versione iniziale.	11 giugno 2021	Non è più supportato.

Connessione mediante un client OpenVPN

È possibile connettersi a un endpoint Client VPN utilizzando le applicazioni client OpenVPN comuni.

> **Note**
>
> Per l'autenticazione federata basata su SAML, per connettersi a un endpoint Client VPN è necessario utilizzare il client fornito da AWS. Per ulteriori informazioni, consulta Connessione mediante un client fornito da AWS o contatta l'amministratore VPN.

Applicazioni client

- Connettiti utilizzando un'applicazione client Windows
- Connessione mediante un'applicazione client VPN per Android o iOS
- Connettiti utilizzando un'applicazione client macOS
- Connessione mediante un'applicazione client OpenVPN

Connettiti utilizzando un'applicazione client Windows

Nelle procedure seguenti viene illustrato come stabilire una connessione VPN utilizzando client VPN basati su Windows.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di Windows.

OpenVPN utilizzando un certificato dall'archivio del sistema di certificati di Windows

È possibile configurare il client OpenVPN in modo che utilizzi un certificato e una chiave privata dall'archivio del sistema di certificati di Windows. Questa opzione è utile quando si utilizza una smart card per la connessione Client VPN. Per informazioni sull'opzione cryptoapicert del client OpenVPN, consulta il Manuale di riferimento per OpenVPN sul sito Web di OpenVPN.

> **Note**
>
> Il certificato deve essere memorizzato nel computer locale.

Per utilizzare l'opzione cryptoapicert con OpenVPN

1. Crea un file con estensione .pfx contenente il certificato client e la chiave privata.
2. Importa il file con estensione .pfx nell'archivio personale dei certificati, sul computer locale. Per ulteriori informazioni, consulta Come visualizzare i certificati con lo snap-in MMC sul sito Web di Microsoft.
3. Verifica che l'account disponga delle autorizzazioni per leggere il certificato sul computer locale. È possibile utilizzare la console di gestione di Microsoft per modificare le autorizzazioni. Per ulteriori informazioni, consulta Diritti per visualizzare l'archivio dei certificati sul computer locale sul sito Web di Microsoft Technet.
4. Aggiorna il file di configurazione OpenVPN e specifica il certificato utilizzando l'oggetto del certificato o l'identificazione personale del certificato.

   Di seguito è riportato un esempio di specifica del certificato utilizzando un oggetto.

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   Di seguito è riportato un esempio di specifica del certificato utilizzando un'identificazione personale. È possibile trovare l'identificazione personale utilizzando la console di gestione di Microsoft. Per ulteriori informazioni, consulta Come recuperare l'identificazione personale di un certificato sul sito Web di Microsoft Technet.

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```

Dopo aver completato la configurazione, utilizza OpenVPN per stabilire una connessione.

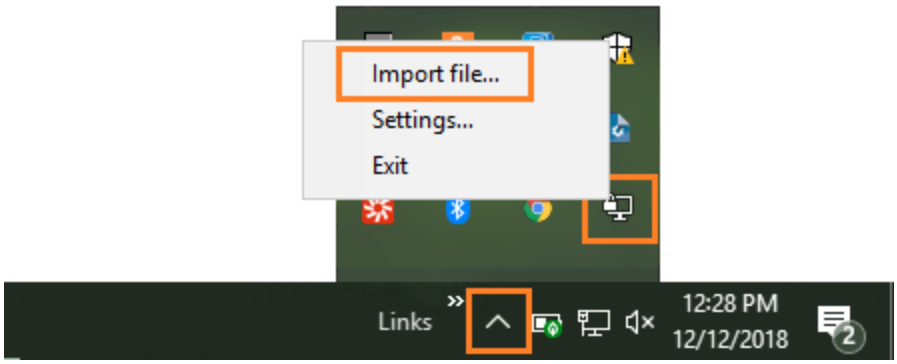
OpenVPN GUI

Nella procedura seguente viene mostrato come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN GUI su un computer Windows.

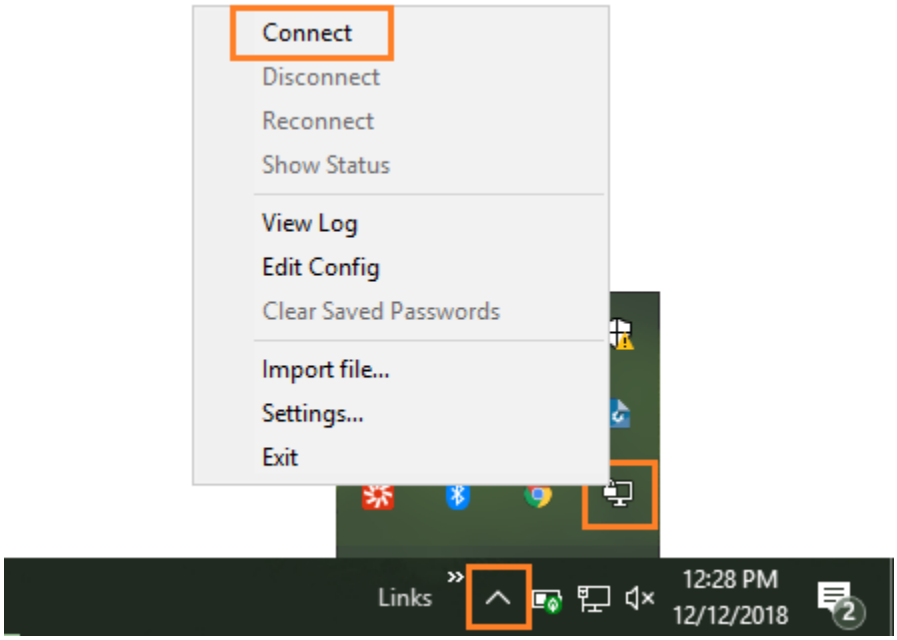
> **Note**
>
> Per informazioni sull'applicazione client OpenVPN, consulta Community Downloads sul sito Web OpenVPN.

Per stabilire una connessione VPN

1. Avviare l'applicazione client OpenVPN.
2. Nella barra delle applicazioni di Windows, scegliere Show/Hide icons (Mostra/Nascondi icone), fare clic con il pulsante destro del mouse su OpenVPN GUI e selezionare Import file (Importa file).



3. Nella finestra di dialogo di apertura, seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Open (Apri).
4. Nella barra delle applicazioni di Windows, scegliere Show/Hide icons (Mostra/Nascondi icone), fare clic con il pulsante destro del mouse su OpenVPN GUI e selezionare Connect (Connetti).



Client OpenVPN Connect

Nella procedura seguente viene mostrato come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN Connect su un computer Windows.

> **Note**
>
> Per ulteriori informazioni, consulta Connecting to Access Server with Windows sul sito Web OpenVPN.

Per stabilire una connessione VPN

1. Avviare l'applicazione client OpenVPN Connect.
2. Nella barra delle applicazioni di Windows, scegliere Show/Hide icons (Mostra/Nascondi icone), fare clic con il pulsante destro del mouse su OpenVPN e selezionare Import profile (Importa profilo).
3. Scegli Import from File (Importa da file) e seleziona il file di configurazione ricevuto dall'amministratore Client VPN.
4. Scegli il profilo di connessione per avviare la connessione.

Connessione mediante un'applicazione client VPN per Android o iOS

La procedura seguente mostra come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN su un dispositivo mobile Android o iOS. I passaggi per Android e iOS sono uguali.

> **Note**
>
> Per ulteriori informazioni sull'applicazione client OpenVPN per Android, consulta le domande frequenti su OpenVPN Connect Android sul sito Web OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Per stabilire la connessione, avvia l'applicazione client OpenVPN, quindi importa il file ricevuto dall'amministratore Client VPN.

Connettiti utilizzando un'applicazione client macOS

Nelle procedure seguenti viene illustrato come stabilire una connessione VPN utilizzando client VPN basati su macOS.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di macOS.

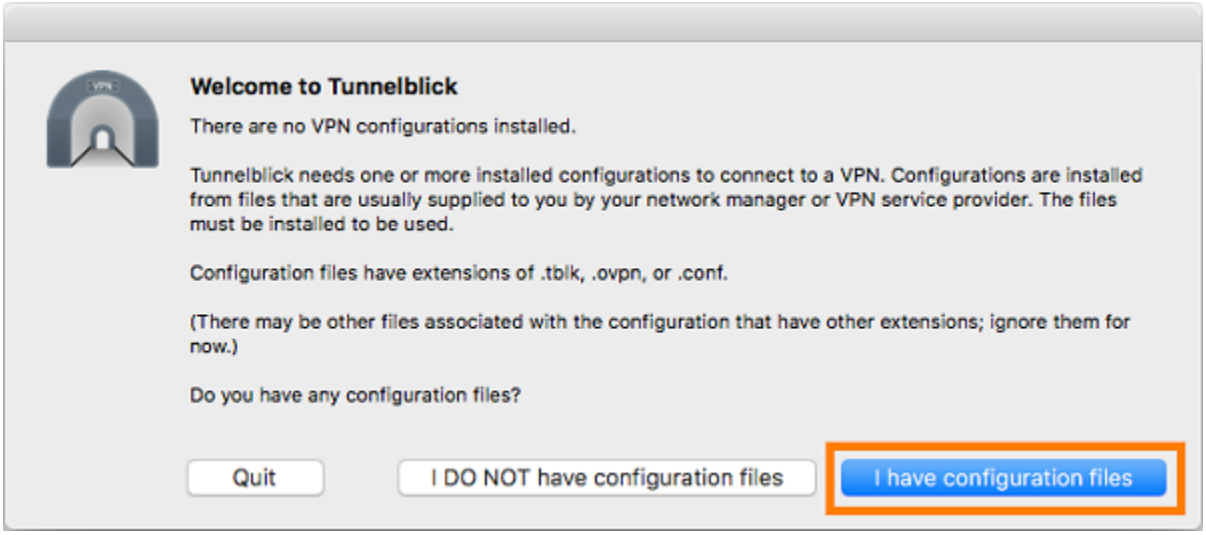
Tunnelblick

La procedura seguente mostra come stabilire una connessione VPN utilizzando l'applicazione client Tunnelblick su un computer macOS.

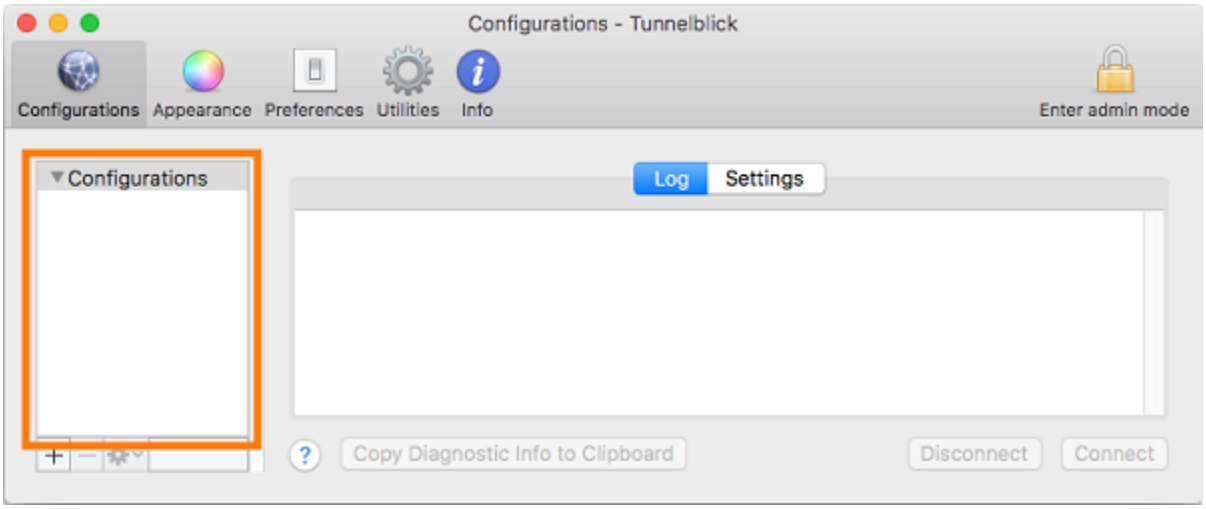
> **Note**
>
> Per ulteriori informazioni sull'applicazione client Tunnelblick per macOS, consulta la documentazione di Tunnelblick sul sito Web Tunnelblick.

Per stabilire una connessione VPN

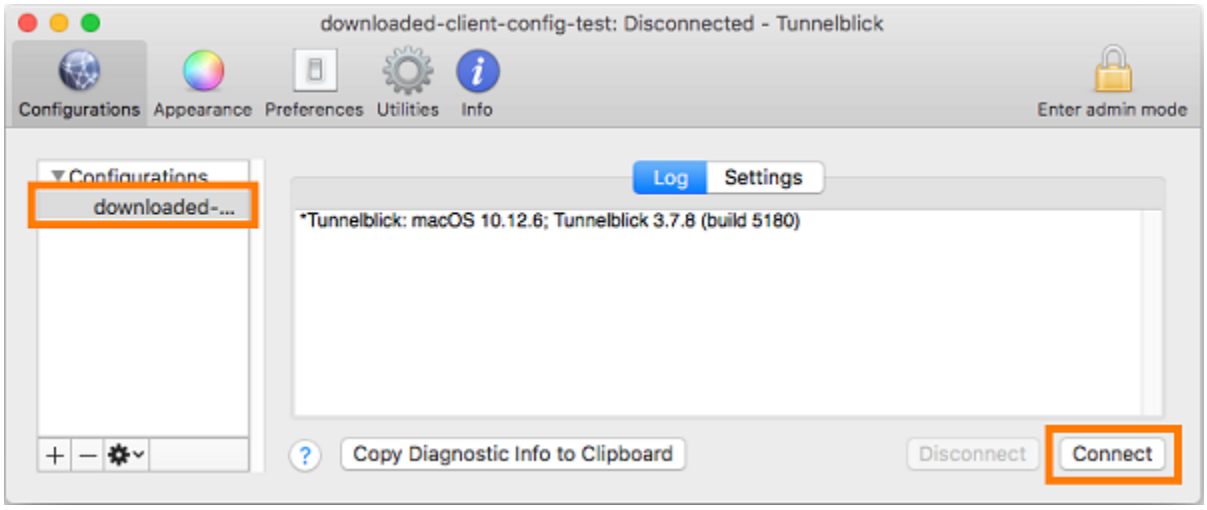
1. Avviare l'applicazione client Tunnelblick e scegliere I have configuration files (Ho i file di configurazione).



2. Trascinare il file di configurazione ricevuto dall'amministratore VPN nel riquadro Configurations (Configurazioni).



3. Selezionare il file di configurazione nel riquadro Configurazioni e scegliere Connetti.



Client OpenVPN Connect

Nella procedura seguente viene mostrato come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN Connect su un computer macOS.

> **Note**
>
> Per ulteriori informazioni, consulta Connecting to Access Server with macOS sul sito Web OpenVPN.

Per stabilire una connessione VPN

1. Avvia l'applicazione OpenVPN e scegli Importa, Dal file locale....
2. Passa al file di configurazione ricevuto dall'amministratore VPN e seleziona Apri.

Connessione mediante un'applicazione client OpenVPN

Nelle procedure seguenti viene illustrato come stabilire una connessione VPN utilizzando client VPN basati su OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia creato un endpoint Client VPN e fornito il file di configurazione dell'endpoint Client VPN.

Per informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi di Linux.

> **Important**
>
> Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione federata basata su SAML, non è possibile utilizzare il client VPN basato su OpenVPN per connettersi a un endpoint Client VPN.

OpenVPN - Gestore di rete

Nella procedura seguente viene mostrato come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN tramite la GUI Network Manager su un computer Windows.

Per stabilire una connessione VPN

1. Installare il modulo Network Manager utilizzando il seguente comando.

   ```
   sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
   ```

2. Passare a Settings (Impostazioni), Network (Rete).
3. Scegliere il simbolo più (+) accanto a VPN, quindi selezionare Import from file... (Importa da file...).
4. Passare al file di configurazione ricevuto dall'amministratore VPN e scegliere Open (Apri).
5. Nella finestra Aggiungi VPN scegli Aggiungi.
6. Avviare la connessione abilitando l'interruttore accanto al profilo VPN aggiunto.

OpenVPN

Nella procedura seguente viene mostrato come stabilire una connessione VPN utilizzando l'applicazione OpenVPN su un computer Ubuntu.

Per stabilire una connessione VPN

1. Installare OpenVPN usando il seguente comando.

   ```
   sudo apt-get install openvpn
   ```

2. Avviare la connessione caricando il file di configurazione ricevuto dall'amministratore VPN.

```
sudo openvpn --config /path/to/config/file
```

Risoluzione dei problemi relativi alla connessione Client VPN

Utilizza gli argomenti seguenti per risolvere i problemi che si potrebbero verificare durante l'utilizzo di un'applicazione client per connettersi a un endpoint Client VPN.

Argomenti

Risoluzione dei problemi degli endpoint Client VPN per gli amministratori

Alcune delle fasi in questa guida possono essere eseguite dall'utente. Altre fasi devono essere eseguite dall'amministratore Client VPN sull'endpoint Client VPN stesso. Nelle sezioni seguenti viene descritto quando è necessario contattare l'amministratore.

Per ulteriori informazioni sulla risoluzione dei problemi relativi agli endpoint Client VPN, consulta Risoluzione dei problemi di Client VPN nella Guida per l'amministratore di AWS Client VPN .

Invia i log di diagnostica AWS Support al client AWS fornito

Se hai problemi con il client AWS fornito e hai bisogno di contattarci per aiutarti AWS Support a risolverli, il client ha la possibilità di inviare i log di diagnostica a. AWS Support L'opzione è disponibile per le applicazioni client Windows, macOS e Linux.

Prima di inviare i file, devi accettare di consentire l'accesso AWS Support ai registri di diagnostica. Dopo aver accettato, ti forniremo un numero di riferimento a cui puoi fornire AWS Support in modo che possano accedere immediatamente ai file.

Invio dei log di diagnostica

Il cliente AWS fornito viene anche chiamato AWS VPN Cliente nei passaggi seguenti.

Per inviare registri di diagnostica utilizzando il client AWS fornito per Windows

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), esegui una delle seguenti operazioni:

   - Per copiare il numero di riferimento negli Appunti, scegli Sì, quindi scegli OK.
   - Per tenere traccia manualmente del numero di riferimento, seleziona No.

   Quando si contatta AWS Support, è necessario fornire loro il numero di riferimento.

Per inviare registri di diagnostica utilizzando il client AWS fornito per macOS

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Prendi nota del numero di riferimento dalla finestra di conferma, quindi scegli OK.

   Quando contatti AWS Support, dovrai fornire loro il numero di riferimento.

Per inviare registri diagnostici utilizzando il client AWS fornito per Ubuntu

1. Apri l'app Client AWS VPN .
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Invia log di diagnostica, scegli Sì.
4. Prendi nota del numero di riferimento dalla finestra di conferma. Se lo desideri, hai la possibilità di copiare le informazioni negli appunti.

   Quando si contatta AWS Support, è necessario fornire loro il numero di riferimento.

Risoluzione dei problemi di Windows

Nelle sezioni seguenti sono riportate informazioni sui problemi che potrebbero verificarsi durante l'utilizzo di client basati su Windows per connettersi a un endpoint Client VPN.

Argomenti

AWS cliente fornito

AWS cliente fornito

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il servizio Windows per eseguire operazioni root. I log dei servizi Windows vengono archiviati nel seguente percorso nel computer.

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

Argomenti

- Impossibile avviare l'applicazione
- Il client non è in grado di creare un profilo
- Si verifica un arresto anomalo del client su PC Dell che utilizzano Windows 10 o 11
- La VPN si disconnette con un messaggio pop-up

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro processo OpenVPN che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Il client non può connettersi con il messaggio di registro “nessun adattatore TAP-Windows”

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN e nei registri delle applicazioni viene visualizzato il seguente messaggio di errore: «Non ci sono adattatori TAP-Windows su questo

sistema. Dovresti essere in grado di creare un adattatore TAP-Windows andando su Avvio -> Tutti i programmi -> TAP-Windows -> Utilità -> Aggiungi un nuovo adattatore Ethernet virtuale TAP-Windows.

Soluzione

È possibile risolvere questo problema eseguendo una o più delle seguenti azioni:

- Riavvia l'adattatore TAP-Windows.
- Reinstalla il driver TAP-Windows.
- Crea un nuovo adattatore TAP-Windows.

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'endpoint Client VPN, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedi all'amministratore Client VPN di verificare che la direttiva `remote` nel file di configurazione venga risolta in un indirizzo IP valido. Puoi anche disconnettere la sessione VPN selezionando Disconnetti nella finestra del client AWS VPN e riprova a connetterti.

Il processo di connessione VPN si chiude in maniera imprevista

Problema

Durante la connessione a un endpoint Client VPN, il client si chiude in maniera imprevista.

Causa

TAP-Windows non è installato sul computer. Questo software è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Impossibile avviare l'applicazione

Problema

In Windows 7, il client AWS fornito non si avvia quando si tenta di aprirlo.

Causa

.NET Framework 4.7.2 o versione successiva non è installato nel computer. Questo è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

```
The config should have either cert and key or auth-user-pass specified.
```

Causa

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

Assicurati che l'amministratore Client VPN aggiunga il certificato e la chiave client al file di configurazione. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .

Si verifica un arresto anomalo del client su PC Dell che utilizzano Windows 10 o 11

Problema

Su alcuni PC Dell (desktop e laptop) che eseguono Windows 10 o 11, è possibile che si verifichi un arresto anomalo durante la navigazione del file system per importare un file di configurazione VPN. Se si verifica questo problema, nei log del client fornito verranno visualizzati messaggi come i seguenti: AWS

```
System.AccessViolationException: Attempted to read or write protected memory. This is
 often an indication that other memory is corrupt.
   at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
 Int32 flags, IntPtr& db)
   at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
 connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
   at System.Data.SQLite.SQLiteConnection.Open()
   at
 STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
 newConnection)
   at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
 targetSettings)
   at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

Causa

Il sistema di backup e ripristino Dell in Windows 10 e 11 potrebbe causare conflitti con il client AWS fornito, in particolare con le seguenti tre DLL:

- DBR .dll ShellExtension
- DBR .dll OverlayIconBackuped
- DBR .dll OverlayIconNotBackuped

Soluzione

Per evitare questo problema, assicurati innanzitutto che il tuo client sia aggiornato con l'ultima versione del client AWS fornito. Vai su Download Client VPN AWS e se è disponibile una versione più recente, esegui l'aggiornamento alla versione più recente.

Devi inoltre eseguire una delle seguenti operazioni:

- Se utilizzi l'applicazione Dell Backup and Recovery, verifica che sia aggiornata. Un post del forum Dell afferma che questo problema è stato risolto nelle versioni più recenti dell'applicazione.
- Se non utilizzi l'applicazione Dell Backup and Recovery, è comunque necessario intraprendere alcune operazioni se si verifica questo problema. Se non desideri aggiornare l'applicazione, in alternativa, è possibile eliminare o rinominare i file DLL. Tuttavia, ricorda che ciò impedirà il funzionamento completo dell'applicazione Dell Backup and Recovery.

Elimina o rinomina i file DLL

1. Accedi a Esplora risorse e individua la posizione in cui è installato Dell Backup and Recovery. In genere è installato nella posizione seguente, ma potrebbe essere necessario cercare per trovarlo.

   ```
   C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
   ```

2. Elimina manualmente i seguenti file DLL dalla directory di installazione o rinominali. Eseguendo entrambe queste operazioni si evita il caricamento.

   - DBR .dll ShellExtension
   - DBR .dll OverlayIconBackuped
   - DBR .dll OverlayIconNotBackuped

   È possibile rinominare i file aggiungendo «.bak» alla fine del nome del file, ad esempio DBR .dll.bak. OverlayIconBackuped

La VPN si disconnette con un messaggio pop-up

Problema

La VPN si disconnette con un messaggio pop-up che dice: «La connessione VPN viene interrotta perché lo spazio degli indirizzi della rete locale a cui è connesso il dispositivo è cambiato. Stabilisci una nuova connessione VPN».

Causa

L'adattatore TAP-Windows non contiene la descrizione richiesta.

Soluzione

Se il `Description` campo non corrisponde a quello riportato di seguito, rimuovi prima l'adattatore TAP-Windows, quindi esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

OpenVPN GUI

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 11.10.0.0 e 11.11.0.0 del software OpenVPN GUI in Windows 10 Home (a 64 bit) e Windows Server 2016 (a 64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

```
C:\Users\User\OpenVPN\config
```

I log di connessione vengono archiviati nel seguente percorso del computer.

```
C:\Users\User\OpenVPN\log
```

Client OpenVPN Connect

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 2.6.0.100 e 2.7.1.101 del software OpenVPN Connect Client in Windows 10 Home (64 bit) e Windows Server 2016 (a 64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

I log di connessione vengono archiviati nel seguente percorso del computer.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

Impossibile risolvere il DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

Causa

Impossibile risolvere il nome DNS. Il client deve anteporre una stringa casuale al nome DNS per impedire la memorizzazione nella cache DNS; tuttavia, alcuni client non lo fanno.

Soluzione

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Alias PKI mancante

Problema

Una connessione a un endpoint Client VPN che non utilizza l'autenticazione reciproca non va a buon fine con il seguente errore.

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

Causa

Il software OpenVPN Connect Client presenta un problema noto in cui tenta di eseguire l'autenticazione utilizzando l'autenticazione reciproca. Se il file di configurazione non contiene una chiave e un certificato client, l'autenticazione non va a buon fine.

Soluzione

Specifica una chiave e un certificato client casuali nel file di configurazione Client VPN e importa la nuova configurazione nel software OpenVPN Connect Client. In alternativa, utilizzare un client diverso, ad esempio il client GUI OpenVPN (v11.12.0.0) o il client Viscosity (v.1.7.14).

Risoluzione dei problemi di macOS

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo dei client macOS. Verifica di eseguire la versione più recente di questi client.

Argomenti

AWS client fornito

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

```
/Users/username/.config/AWSVPNClient/logs
```

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il demone client per eseguire operazioni root. I log del daemon vengono archiviati nei seguenti percorsi del computer.

```
/tmp/AcvcHelperErrLog.txt
/tmp/AcvcHelperOutLog.txt
```

Il client AWS fornito memorizza i file di configurazione nella seguente posizione sul computer.

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

Argomenti

- Il client non è in grado di connettersi
- Il client è bloccato in uno stato di riconnessione
- Il client non è in grado di creare un profilo

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro processo OpenVPN che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'endpoint Client VPN, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedi all'amministratore Client VPN di verificare che la direttiva `remote` nel file di configurazione venga risolta in un indirizzo IP valido. Puoi anche disconnettere la sessione VPN selezionando Disconnetti nella finestra del client AWS VPN e riprova a connetterti.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

```
The config should have either cert and key or auth-user-pass specified.
```

Causa

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

Assicurati che l'amministratore Client VPN aggiunga il certificato e la chiave client al file di configurazione. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .

Tunnelblick

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 3.7.8 (build 5180) del software Tunnelblick su macOS High Sierra 10.13.6.

Il file di configurazione per le configurazioni private viene archiviato nel seguente percorso del computer.

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

Il file di configurazione per le configurazioni condivise viene archiviato nel seguente percorso del computer.

```
/Library/Application Support/Tunnelblick/Shared
```

I log di connessione vengono archiviati nel seguente percorso del computer.

```
/Library/Application Support/Tunnelblick/Logs
```

Per aumentare il dettaglio dei log, aprire l'applicazione Tunnelblick, scegliere Settings (Impostazioni) e regolare il valore per VPN log level (Livello di log VPN).

Impossibile trovare l'algoritmo di cifratura 'AES-256-GCM'

Problema

La connessione non riesce e restituisce il seguente errore nei log.

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

Causa

L'applicazione utilizza una versione OpenVPN che non supporta l'algoritmo di crittografia AES-256-GCM.

Soluzione

Scegliere una versione di OpenVPN compatibile nel modo seguente:

1. Aprire l'applicazione Tunnelblick.

2. Seleziona Impostazioni.
3. Per OpenVPN version (Versione di OpenVPN), scegliere 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - la versione OpenSSL è v1.0.2q).

La connessione smette di rispondere e si ripristina

Problema

La connessione non riesce e restituisce il seguente errore nei log.

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

Causa

Il certificato client è stato revocato. La connessione smette di rispondere dopo aver tentato di autenticarsi e alla fine viene ripristinata dal lato server.

Soluzione

Richiedi un nuovo file di configurazione dall'amministratore Client VPN.

Utilizzo chiave esteso (EKU)

Problema

La connessione non riesce e restituisce il seguente errore nei log.

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
```

```
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

Causa

L'autenticazione del server è stata completata. Tuttavia, l'autenticazione client non va a buon fine perché il campo Utilizzo chiave esteso (EKU) del certificato client è abilitato per l'autenticazione del server.

Soluzione

Verifica di utilizzare il certificato e la chiave client corretti. Se necessario, verifica con l'amministratore VPN Client. Questo errore può verificarsi se usi il certificato server e non il certificato client per connetterti all'endpoint Client VPN.

Certificato scaduto

Problema

L'autenticazione del server va a buon fine ma l'autenticazione client non riesce con il seguente errore.

```
WARNING: “Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
 process restarting”
```

Causa

La validità del certificato client è scaduta.

Soluzione

Richiedi un nuovo certificato client all'amministratore Client VPN.

OpenVPN

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 2.7.1.100 del software OpenVPN Connect Client su macOS High Sierra 10.13.6.

Il file di configurazione viene archiviato nel seguente percorso del computer.

```
/Library/Application Support/OpenVPN/profile
```

I log di connessione vengono archiviati nel seguente percorso del computer.

```
Library/Application Support/OpenVPN/log/connection_name.log
```

Impossibile risolvere DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

Causa

OpenVPN Connect non è in grado di risolvere il nome DNS Client VPN.

Soluzione

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Risoluzione dei problemi di Linux

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo di client basati su Linux. Verifica di eseguire la versione più recente di questi client.

Argomenti

- AWS cliente fornito
- OpenVPN (riga di comando)

- OpenVPN tramite Network Manager (GUI)

AWS cliente fornito

Il client AWS fornito archivia i file di registro e i file di configurazione nella seguente posizione sul sistema:

```
/home/username/.config/AWSVPNClient/
```

Il processo daemon client AWS fornito archivia i file di registro nella seguente posizione sul sistema:

```
/var/log/aws-vpn-client/username/
```

Problema

In alcuni casi, dopo aver stabilito una connessione VPN, le query DNS continueranno a passare al server dei nomi di sistema predefinito anziché ai server dei nomi configurati per l'endpoint Client VPN.

Causa

Il Client interagisce con systemd-resolved, un servizio disponibile sui sistemi Linux, che funge da elemento centrale della gestione DNS. Viene utilizzato per configurare i server DNS che vengono spinti dall'endpoint Client VPN. Il problema si verifica perché systemd-resolved non imposta la priorità più alta per i server DNS forniti dall'endpoint Client VPN. Al contrario, i server vengono aggiunti all'elenco esistente dei server DNS configurati nel sistema locale. Di conseguenza, i server DNS originali potrebbero ancora avere la priorità più alta e quindi essere utilizzati per risolvere le query DNS.

Soluzione

1. Aggiungi la seguente direttiva nel file di configurazione di OpenVPN per essere certo che tutte le query DNS vengano inviate nel tunnel VPN.

   ```
   dhcp-option DOMAIN-ROUTE .
   ```

2. Utilizza il resolver stub fornito da systemd-resolved. Per far ciò, collegare simbolicamente `/etc/resolv.conf` a `/run/systemd/resolve/stub-resolv.conf` emettendo il seguente comando sul sistema.

```
sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
```

3. (Facoltativo) Se non vuoi che systemd-resolved utilizzi un proxy per le query DNS ma desideri che le query vengano inviate direttamente ai server dei nomi DNS reali, stabilisci un collegamento simbolico da `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`.

   ```
   sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

   Questa procedura può essere necessaria per bypassare systemd-resolved, ad esempio per la memorizzazione nella cache delle risposte DNS, la configurazione DNS per interfaccia, l'imposizione DNSSec e così via. Questa opzione è particolarmente utile quando è necessario sovrascrivere un record DNS pubblico con un record privato quando si è connessi a VPN. Ad esempio, è possibile che nel VPC privato sia presente un resolver DNS privato con un record per www.example.com, che viene risolto in un IP privato. Questa opzione può essere utilizzata per sovrascrivere il record pubblico di www.example.com, che si risolve in un IP pubblico.

OpenVPN (riga di comando)

Problema

La connessione non funziona correttamente perché la risoluzione DNS non funziona.

Causa

Il server DNS non è configurato nell'endpoint Client VPN o non viene accettato dal software client.

Soluzione

Utilizzare le fasi seguenti per verificare che il server DNS sia configurato e funzioni correttamente.

1. Accertarsi che una voce del server DNS sia presente nei log. Nell'esempio seguente, il server DNS `192.168.0.2` (configurato nell'endpoint Client VPN) viene restituito nell'ultima riga.

   ```
   Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
   WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
    'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
   gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
    10.0.0.98 255.255.255.224,peer-id 0
   ```

Se non è specificato alcun server DNS, chiedi all'amministratore Client VPN di modificare l'endpoint Client VPN assicurandosi che per l'endpoint Client VPN sia specificato un server DNS (ad esempio il server DNS VPC). Per ulteriori informazioni, consulta Endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

2. Per accertarsi che il pacchetto `resolvconf` sia installato, eseguire il comando seguente.

```
sudo apt list resolvconf
```

Viene restituito l'output seguente.

```
Listing... Done
resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
```

Se non è installato, installarlo utilizzando il seguente comando.

```
sudo apt install resolvconf
```

3. Apri il file di configurazione Client VPN (il file.ovpn) in un editor di testo e aggiungi le seguenti righe.

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

Controllare i log per verificare che lo script `resolvconf` sia stato richiamato. I log devono contenere una riga simile alla seguente.

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

OpenVPN tramite Network Manager (GUI)

Problema

Quando si utilizza il client Network Manager OpenVPN, la connessione non riesce con il seguente errore.

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

Causa

Il flag `remote-random-hostname` non è rispettato e il client non può connettersi utilizzando il pacchetto `network-manager-gnome`.

Soluzione

Consulta la soluzione Impossibile risolvere il nome DNS dell'endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Problemi comuni

Di seguito sono riportati i problemi comuni che possono verificarsi quando utilizzi un client per connetterti a un endpoint Client VPN.

Negoziazione chiave TLS non riuscita

Problema

La negoziazione TLS non va a buon fine con il seguente errore.

```
TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
TLS Error: TLS handshake failed
```

Causa

La causa del problema può essere una delle seguenti:

- Le regole del firewall bloccano il traffico UDP o TCP.
- La chiave e il certificato client utilizzati nel file di configurazione (.ovpn) sono errati.
- L'elenco di revoche di certificati (CRL) del client è scaduto.

Soluzione

Verifica che le regole del firewall sul computer non blocchino il traffico TCP o UDP in ingresso o in uscita sulle porte 443 o 1194. Chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Le regole del firewall per l'endpoint Client VPN non blocchino il traffico TCP o UDP sulle porte 443 o 1194.
- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta Esportazione della configurazione client nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta Il client non è in grado di connettersi a un endpoint Client VPN nella Guida per l'amministratore di AWS Client VPN .

Cronologia dei documenti

La tabella seguente descrive gli aggiornamenti della AWS Client VPN User Guide.

Modifica	Descrizione	Data
AWS rilasciato il client fornito (3.9.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.11.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	19 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.10.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.8.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.10.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023

AWS rilasciato il client fornito (3.9.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.8.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.7.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.8.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.5.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.5.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.3.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	27 aprile 2023

AWS rilasciato il client fornito (3.5.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 aprile 2023
AWS rilasciato il client fornito (3.4.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	28 marzo 2023
AWS rilasciato il client fornito (3.3.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2023
AWS rilasciato il client fornito (3.4.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 febbraio 2023
AWS rilasciato il client fornito (3.2.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.2.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (2.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022

AWS rilasciato il client fornito (2.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (2.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (1.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	9 novembre 2021
AWS rilasciato il client fornito per Windows (1.3.7)	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.3) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	28 settembre 2021
AWS rilasciato il client fornito per Windows (1.3.6) e macOS (1.3.5)	Per informazioni dettagliate, consulta le note di rilascio.	20 settembre 2021
AWS rilasciato il client fornito per Ubuntu 18.04 LTS e Ubuntu 20.04 LTS	È possibile utilizzare il AWS client fornito su Ubuntu 18.04 LTS e Ubuntu 20.04 LTS.	11 giugno 2021
Supporto per OpenVPN tramite un certificato dall'archivio del sistema di certificati di Windows	Puoi utilizzare OpenVPN con un certificato dall'archivio del sistema di certificati di Windows	25 febbraio 2021
Portale self-service	È possibile accedere a un portale self-service per ottenere il client e il file di configurazione più recenti AWS forniti.	29 ottobre 2020

AWS cliente fornito	È possibile utilizzare il client AWS fornito per connettersi a un endpoint Client VPN.	4 febbraio 2020
Versione iniziale	Questa versione introduce AWS Client VPN.	18 dicembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.